

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-123144

(43)Date of publication of application : 28.04.2000

(51)Int.Cl. G06K 19/10
 B42D 15/10
 G06K 19/07
 G06K 19/06

(21)Application number : 10-290572

(71)Applicant : SONY CORP

(22)Date of filing : 13.10.1998

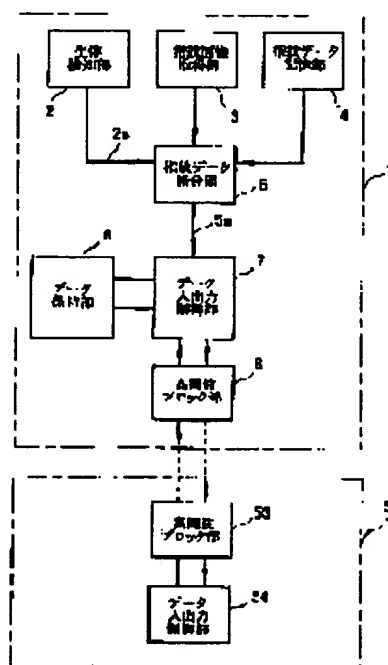
(72)Inventor : IMAGAWA TOSHIYUKI

(54) CONTACTLESS IC CARD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contactless IC card which can surely discriminate its genuine user and also can improve its security.

SOLUTION: This contactless IC card includes a fingerprint acquisition part 3 which detects the fingerprint image of a finger, a fingerprint data storage part 4 which stores the fingerprint data on a specific finger, a data input/output control part 7 which performs the contactless input/output of data to an external device, a high frequency block part 8 and a fingerprint data collation part 5 which collates the detected fingerprint data with the stored ones and permits the input/output of data to the external device only when the coincidence is confirmed between both fingerprint data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-123144

(P2000-123144A)

(43) 公開日 平成12年4月28日 (2000.4.28)

(51) Int.Cl. ⁷	識別記号	F I	マークト* (参考)
G 0 6 K 19/10		G 0 6 K 19/00	S 2 C 0 0 5
B 4 2 D 15/10	5 2 1	B 4 2 D 15/10	5 2 1 5 B 0 3 5
G 0 6 K 19/07		G 0 6 K 19/06	
19/06		19/00	H

審査請求 未請求 請求項の数 8 O L (全 8 頁)

(21) 出願番号 特願平10-290572

(22) 出願日 平成10年10月13日 (1998.10.13)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 今川 敏幸

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100094053

弁理士 佐藤 隆久

Fターム(参考) 2C005 MA03 NA09 SA05 SA15 TA22

5B035 AA14 CA11 CA12 CA23 CA26

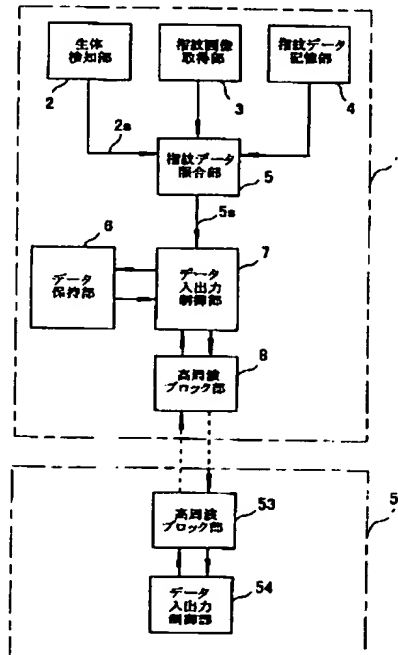
CA38

(54) 【発明の名称】 非接触式 I C カード

(57) 【要約】

【課題】 I C カードの真正の利用者の判別が確実に可能で、セキュリティの向上した非接触式 I C カードを提供する。

【解決手段】 指の指紋画像を検出する指紋画像取得部 3 と、特定指の指紋データを記憶保持する指紋データ記憶部 4 と、外部機器との間で非接触でデータの入出力を行うデータ入出力制御部 7 および高周波ブロック部 8 と、検出された指紋データと記憶された指紋データとを照合し、両者が合致する場合にのみ外部機器とのデータの入出力を許可する指紋データ照合部 5 とを有する。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 指の指紋画像を検出する指紋画像検出手段と、
特定指の指紋データを記憶保持する指紋データ記憶手段と、
外部機器との間で非接触でデータの入出力を行うデータ入出力手段と、
検出された指紋データと記憶された指紋データとを照合し、両者が合致する場合にのみ外部機器とのデータの入出力を許可する照合手段とを有する非接触式ＩＣカード。

【請求項2】 前記指紋画像検出手段は、前記カードの所定の位置に形成され、指紋画像を検出する指紋画像検出素子と、
前記指紋画像検出素子によって得られた指紋画像データに所定の処理を施す画像処理回路とを有する請求項1に記載の非接触式ＩＣカード。

【請求項3】 前記指紋画像検出手段によって検出される検出対象物が生体であるか否かを検出する生体検知手段と、
前記生体検知手段の検出信号に基づいて前記照合手段による照合を許可するか否かを判断する判断手段とをさらに有する請求項1に記載の非接触式ＩＣカード。

【請求項4】 前記生体検知手段は、前記ＩＣカードの利用者の指の有する静電容量を検出する静電容量検出手段である請求項3に記載の非接触式ＩＣカード。

【請求項5】 前記静電容量検出手段は、カードの表面に形成された複数の静電容量検出用電極パターンと、
前記各静電容量検出用電極パターン間に形成された静電容量を検出する静電容量検出回路とを有する請求項4に記載の非接触式ＩＣカード。

【請求項6】 前記静電容量検出手段は、ＩＣカードの表面の前記指紋画像検出素子の周囲に隣接して形成された複数の静電容量検出用電極パターンと、
前記各静電容量検出用電極パターン間に形成される静電容量を検出する静電容量検出回路とを有する請求項4に記載の非接触式ＩＣカード。

【請求項7】 前記判断手段は、前記検出された静電容量の大きさに基づいて、前記照合手段による照合の許可を判断する請求項4に記載の非接触式ＩＣカード。

【請求項8】 ＩＣカードに内蔵された各回路を駆動する電力を前記外部機器から非接触で受給可能な電力供給手段をさらに有する請求項1に記載の非接触式ＩＣカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、外部機器との間で非接触でデータの入出力が可能な非接触式ＩＣカードに関する。

【0002】

【従来の技術】 たとえば、マイクロプロセッサやメモリを構成する集積回路が埋め込まれたＩＣカードには、外部端子付きの接触式ＩＣカードと、外部端子を有しない非接触式ＩＣカードが知られており、非接触式ＩＣカードは外部機器に直接接続する必要がないため操作性が良い等の利点を有する。一方、ＩＣカードでは、ＩＣカードの不正利用を防ぐために、ＩＣカードの利用者が真正の利用者であるかを判断するための方法が種々提案され、ＩＣカードのセキュリティの向上が図られている。利用者本人であることを確認する方法として、たとえば、ＩＣカードとの間でデータのやり取りを行う外部機器であるリーダライタに利用者が暗証番号を入力する方法が知られている。この方法では、ＩＣカードに記憶された暗証番号は、ＩＣカードをリーダライタに挿入するとリーダライタに読み込まれ、リーダライタに利用者によって入力された暗証番号と比較される。両方の暗証番号が一致すると利用者はＩＣカードを利用することができる。

【0003】

【発明が解決しようとする課題】 しかしながら、上記の方法では、ＩＣカードの利用者が真正の利用者でない場合にも、利用者が当該ＩＣカードに記憶されている暗証番号を知得していればＩＣカードを利用することができるため、セキュリティの面からは十分ではない。また、外部機器に対して暗証番号を入力する構成とすると、非接触式のＩＣカードの外部機器との間で非接触で操作でき、操作性が良いという利点が損なわれる。

【0004】 また、ＩＣカードの利用者が真正の利用者であるかを判断するために、真正の利用者の特定指の指紋を外部機器であるリーダライタの管理者が予め登録しておき、ＩＣカードの利用の際に、利用者の指紋と登録された指紋とを照合する方法も考えられる。しかしながら、この方法では、リーダライタの管理者が指紋情報を管理し、かつ、指紋を照合するため、たとえば、リーダライタの管理者によって登録された指紋情報を用いてＩＣカード内のデータが改ざんされたり、登録された指紋情報を入手した不正利用者が指紋情報のコピー（模造型）を作成してＩＣカードを不正利用する等のおそれがある。

【0005】 本発明は、上記問題に鑑みてなされたものであって、ＩＣカードの真正の利用者の判別が確実に可能で、セキュリティの向上した非接触式のＩＣカードを提供することを目的とする。

【0006】

【課題を解決するための手段】 本発明は、指の指紋画像を検出する指紋画像検出手段と、特定指の指紋データを記憶保持する指紋データ記憶手段と、外部機器との間で非接触でデータの入出力を行うデータ入出力手段と、検出された指紋データと記憶された指紋データとを照合し、両者が合致する場合にのみ外部機器とのデータの入

出力を許可する照合手段とを有する。

【0007】前記指紋画像検出手段は、前記カードの所定の位置に形成され、指紋画像を検出する指紋画像検出素子と、前記指紋画像検出素子によって得られた指紋画像データに所定の処理を施す画像処理回路とを有する。

【0008】前記指紋画像検出手段によって検出される検出対象物が生体であるか否かを検出する生体検知手段と、前記生体検知手段の検出信号に基づいて前記照合手段による照合を許可するか否かを判断する判断手段とをさらに有する。

【0009】前記生体検知手段は、前記ICカードの利用者の指の有する静電容量を検出する静電容量検出手段である。

【0010】前記静電容量検出手段は、カードの表面に形成された複数の静電容量検出用電極パターンと、前記各静電容量検出用電極パターン間に形成された静電容量を検出する静電容量検出回路とを有する。

【0011】前記静電容量検出手段は、ICカードの表面の前記指紋画像検出素子の周囲に隣接して形成された複数の静電容量検出用電極パターンと、前記各静電容量検出用電極パターン間に形成される静電容量を検出する静電容量検出回路とを有する。

【0012】前記判断手段は、前記検出された静電容量の大きさに基づいて、前記照合手段による照合の許可を判断する。

【0013】ICカードに内蔵された各回路を駆動する電力を前記外部機器から非接触で受給可能な電力供給手段をさらに有する。

【0014】本発明では、指紋画像検出手段によってICカードの利用者の指紋を検出し、予めICカードの指紋データ記憶手段に記憶されていた真正な利用者の指紋データと照合し、両者が合致すると外部機器との間で非接触でデータの入出力が可能になる。

【0015】また、本発明では、ICカードの接触した指が生体検知手段によって生体か否かを検知され、生体である場合にのみ検出された指紋データと真正な利用者の指紋データとの照合を行う。このため、ICカードの真正の利用者の指紋を模造してICカードを利用することを防止することができる。

【0016】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図1は、本発明の一実施形態に係るICカードの構成を示す構成図である。図1に示すICカード1は、生体検知部2と、指紋画像取得部3と、指紋データ記憶部4と、指紋データ照合部5と、データ保持部6と、データ入出力制御部7と、高周波ブロック部8とを有する。

【0017】生体検知部2は、ICカード1の利用者の指紋画像データを取得する際に、検出対象の指が人体

(生体)であるか否かを検出する。生体検知部2は、生

体を検知した場合に、指紋データ照合部5に対して検知信号2sを出力する。指紋画像取得部3は、ICカード1の利用者の指紋画像データを取得し、当該指紋画像データに、たとえば、2値化処理等の所定の処理を施して、指紋データを取得する。指紋データ記憶部4は、ICカード1の真正の利用者の指紋データを予め記憶保持する。指紋データは、真正の利用者の特定の指、たとえば、人指し指の指紋データである。

【0018】指紋データ照合部5は、指紋データ記憶部4に記憶保持された真正の利用者の指紋データと指紋画像取得部3によって取得されたICカード1の利用者の指紋データとを照合する。指紋データ照合部5は、真正の利用者の指紋データと取得された利用者の指紋データとが合致する場合には、データ入出力制御部7に対して許可信号5sを出力する。また、指紋データ照合部5は、生体検知部2からの検知信号2sが入力された場合にのみ、真正の利用者の指紋データと取得された利用者の指紋データとの照合を行う。

【0019】データ保持部6は、外部機器との間で入出力される各種データを記憶保持し、たとえば、ICカード1が電子決済に使用される場合には、真正の利用者の口座情報、金銭の取引情報等が記憶されたり、IDカードとして使用される場合には、各種の個人情報等が記憶される。

【0020】データ入出力制御部7は、指紋データ照合部5から入力される許可信号5sに応じて、外部機器51との間で各種データの入出力を行う。データ入出力制御部7は、たとえば、指紋データ照合部5から許可信号5sが入力されると、すなわち、ICカード1の利用者が真正の利用者であると判断されると、外部機器51に対して出力すべきデータをデータ保持部6から読みだして高周波ブロック部8に出力したり、外部機器51から高周波ブロック部8を通じて入力されるデータを読み込んでデータ保持部6に書き込む作業を行う。

【0021】高周波ブロック部8は、データ入出力制御部7から出力されたデータを高周波信号に変調し、これを高周波の電磁波として外部機器51の有する高周波ブロック部53に対して無線方式で送信する。また、高周波ブロック部8は、外部機器51の高周波ブロック部53から送信されてきた電磁波からなる高周波信号を復調し、所定のデータ形式に変換してデータ入出力制御部7に出力する。さらに、高周波ブロック部8は、外部機器51の高周波ブロック部53から送られてくる電磁波としての交流電力を整流してICカード1の有する各回路に必要な電源を供給する。

【0022】外部機器51は、高周波ブロック部53と、データ入出力制御部54とを有しており、また、外部機器51は、たとえば、ネットワーク手段によってICカード1の管理者またはデータ通信を行う者との間で接続されている。外部機器51のデータ入出力制御部5

4は、高周波ブロック部53を介したICカード1との間のデータの入出力動作を制御し、たとえば、ネットワーク手段を介して外部機器51に送信されたデータがデータ入出力制御部54に入力されたり、高周波ブロック部53を通じてICカード1から送信されたデータが入力される。また、高周波ブロック部53は、外部機器51に設けられた交流電源からの交流電力を電磁波としてICカード1の高周波ブロック部8に供給する。

【0023】図2は、上記構成のICカード1を実現するハードウェア構成の一例を示す構成図である。図2において、ICカード1は、指紋画像検出素子11と、指紋画像処理回路15と、メモリ16と、静電容量検出回路17と、静電容量検出用電極19と、マイクロプロセッサ21と、インターフェース回路22と、送受信回路23とを有している。また、外部機器51は、送受信回路55と、コントロールユニット56と、交流電源57とを有している。

【0024】指紋画像検出素子11は、ICカード1の利用者の特定の指の指紋画像を検出するための素子である。指紋画像検出素子11は、たとえば、図3に示すように、ICカード1の表面に形成された指紋画像検出領域R内の中央位置に形成されている。指紋画像検出領域Rは、たとえば、図4に示すように、指Fを載せやすいように、指Fの先端の大きさに適合した大きさで、かつ、ICカード1の表面から所定の高さで突出した形状に形成することができる。指紋画像検出素子11には、たとえば、CCD(Charge Coupled Device)素子を用いることができる。

【0025】また、指紋画像検出素子11として、たとえば、図6に示すように、X軸およびY軸方向に沿って所定間隔で複数のパターンpxおよびpyが形成され、これら各パターンpxおよびpyの各交差点Kの静電容量を検出するための静電容量検出回路を備えたICチップ11によっても、指紋画像を検出することができる。人間の指は、たとえば、150~200μm程度の高さの凹凸で指紋を形成しており、ICチップ11のパターンpxおよびpyの形成面に指を接触させると、指の凹凸によってICチップ11のパターンpxおよびpyの各交差点Kにおける静電容量は凹凸の高さに応じた値となる。したがって、各交差点Kにおける静電容量を検出し、各交差点Kにおける静電容量の大きさをたとえば2値化処理することにより、指紋データに変換することができる。

【0026】指紋画像処理回路15は、ICカード1内に内蔵され、上記の指紋画像検出素子11によって所得された指紋画像データに対して所定の処理を施して指紋データに変換する。なお、指紋画像検出素子11および指紋画像処理回路15によって、上記の指紋画像取得部3が構成される。

【0027】静電容量検出用電極19は、ICカード1

の利用者の指Fの有する静電容量を検出するための複数の電極からなり、たとえば、図3に示すように、指紋画像検出素子11の周囲に隣接してX軸およびY軸方向に沿って、2つの電極19aおよび19bがICカード1の表面に露出するように形成される。電極19a間および電極19b間に形成される指の静電容量Cxは、たとえば、静電容量検出回路17によって検出される。

【0028】静電容量検出回路17は、ICカード1に内蔵されており、たとえば、図5に示すような、静電容量検出用電極19によって検出される静電容量Cxの大きさに応じた電流(電圧)を発生させる回路から構成される。図5に示す静電容量検出回路17は、いわゆるウィーンブリッジ回路から基本的に構成されており、端子Paと端子Pbとの間および端子Paと端子Pdとの間に既知の抵抗Q、Pが接続され、端子Pbと端子Pcとの間に可変抵抗Rと可変コンデンサCが直列に接続されている。端子Pcと端子Pdとの間には、上記の各静電容量検出用電極19aまたは19bの間に形成される絶縁抵抗や漏洩抵抗等の抵抗Rxが形成されるとともに、この抵抗Rxに並列に各静電容量検出用電極19aまたは19bの間の静電容量Cxが形成される。また、端子Pbと端子Pdの間には検流回路Dが接続され、端子Paと端子Pcの間には発振器OSCが接続されている。

【0029】発振器OSCは、所定の周波数の電圧信号を端子Paと端子Pcとの間に印加する。発振器OSCは、たとえば、ICカード1内に内蔵されており、外部機器51から送られる電力によって所定周波数のクロック信号を発生する。検流回路Dは、端子Pbと端子Pdとの間に流れる電流を検出する回路であるが、たとえば、A/D変換回路から構成することができる。

【0030】上記構成の静電容量検出回路17は、静電容量検出用電極19aおよび19bに対してそれぞれ設けるが、たとえば、単一の静電容量検出回路17を切り換えて静電容量検出用電極19aおよび19bの検出する各静電容量Cxを検出する構成としてもよい。上記構成の静電容量検出回路17では、ICカード1の表面に形成された静電容量検出用電極19aおよび19bに指が接触していない状態で、たとえば、検流回路Dに電流が流れないように、可変抵抗Rおよび可変抵抗Cを調整しておく。この状態で、ICカード1の表面に形成された静電容量検出用電極19aおよび19bに指が接触すると、指の静電容量Cxに応じた大きさの電流が検流回路Dに流れ、検流回路Dではこの電流値をデジタル変換する。したがって、上記構成の静電容量検出回路17では、指の静電容量Cxに応じた大きさの電流値がデジタル値で得られる。

【0031】メモリ16は、上記の指紋データ記憶部4およびデータ保持部6を構成しており、たとえば、EPROM(Erasable PROM)やEEPROM(Electrically E

erasable PROM)等の書き換え可能なメモリで構成することができる。メモリ16へのデータの書き込みは、外部機器51から送信される書き込み電圧 V_{pp} によって行われる。

【0032】マイクロプロセッサ21は、内部に、制御演算回路部21a、ROM21bおよびRAM21cを有している。ROM21bは、ICカード1で行う各種処理を規定したプログラムを記憶しており、ICカード1の機能はこのプログラムで決定される。たとえば、上記した指紋データ照合部5の指紋データの照合等の処理を行うプログラムは、あらかじめROM21bに記憶されている。RAM21cは、ROM21bに記憶されたプログラムデータや、制御演算回路部21aで算出したデータや、インターフェース回路22から入力されたデータや、指紋画像処理回路15から出力された指紋データを一時的に保持するメモリである。制御演算回路部21aは、ROM21bに記憶されたプログラムを実行し、各種の演算動作、周辺回路の制御動作を行う。

【0033】インターフェース回路22は、送受信回路23を通じて入力される入力データ、たとえば、シリアルデータをパラレルデータに変換してマイクロプロセッサ21の制御演算回路部21aに入力し、制御演算回路部21aから出力されたパラレルデータをシリアルデータに変換して送受信回路23に出力する。

【0034】送受信回路23は、外部機器51の送受信回路55から電力を受信するとともに、送受信回路55との間で各種データの送受信を行う回路である。送受信回路23は、たとえば、コイルとコンデンサを有する同調回路と、変調回路、復調回路、整流回路等の回路から構成することができる。インターフェース回路22から送受信回路23に出力されたデータは、送受信回路23の変調回路によって変調され、同調回路で発生される高周波電磁波に乗って外部機器51の送受信回路55に送信される。また、送受信回路23の同調回路は、外部機器51の送受信回路55から送信されてくる高周波電磁波を受信し、電磁誘導作用による起電力を整流回路で直流電力に変換したのち、コンデンサに蓄える。コンデンサに蓄えられた電力によって、ICカード1に内蔵された各回路が駆動される。さらに、送受信回路23は、外部機器51の送受信回路55から送信されてくる高周波電磁波に乗ったデータを受信して、送受信回路23の復調回路で変調されたデータを復調し、インターフェース回路22に出力する。

【0035】外部機器51の送受信回路55は、コイルとコンデンサを具備する同調回路を有しており、交流電源57を供給源として、交流電力を電磁波でICカード1の送受信回路23に送信する。また、外部機器51のコントロールユニット56から出力されるデータを変調し、電磁波に乗せてICカード1の送受信回路23に送信する。さらに、外部機器51の送受信回路55の受信

したデータを復調してコントロールユニット56に出力する。

【0036】上記構成のICカード1では、まず、指紋データ記憶部4に真正な利用者の特定指の指紋データを登録する必要がある。真正な利用者の指紋データの登録は、たとえば、マイクロプロセッサ21のROM21bに、指紋データの登録のためのプログラムを内蔵しておき、ICカード1の初めての利用の際にICカード1を外部機器51の近くにかざすと、ICカード1に電力が供給され、指紋データの登録のためのプログラムが動作するようにしておく。ICカード1の利用者が特定指をICカード1の表面に形成された指紋画像検出領域R内の指紋画像検出素子11に密着させると、指紋画像処理回路15を通じて得られた指紋データがマイクロプロセッサ21からメモリ16の所定のアドレスに記憶される構成とすることができる。また、上記のように、ICカード1に指紋データの登録のためのプログラムを内蔵させるのではなく、外部機器51側に用意しておき、外部機器51からICカード1に電力を送信するとともに、指紋データの登録のためのプログラムデータを送信する構成とすることも可能である。

【0037】次に、上記構成のICカードの使用方法の一例について、図7に示すフローチャートに基づいて説明する。まず、ICカード1を所定の外部機器51に対して電磁波による電力を受信可能な位置に近づける(ステップS1)。ICカード1には、外部機器51の送受信回路55から電磁波により電力が供給される(ステップS2)。これにより、ICカード1の指紋画像処理回路15およびマイクロプロセッサ21には電源電圧が供給される。また、外部機器51の送受信回路55から電磁波に乗ってリセット信号RSTが送信され、インターフェース回路22を通じてマイクロプロセッサ21に入力されることによりマイクロプロセッサ21が動作可能な状態となる。さらに、静電容量検出回路17には発振器OSCからのクロック信号が供給され、静電容量検出回路17は静電容量Cxを検出可能な状態となる。

【0038】次いで、ICカード1の利用者は、ICカード1に形成された指紋画像検出領域Rに特定の指を密着させる(ステップS3)。指紋画像検出領域R内に形成された静電容量検出用電極19aおよび/または19bに指が接触し、静電容量検出回路17の検流回路Dに静電容量Cxの大きさに応じた電流が流れ、この電流が検出される(ステップS4)。検出された電流値は、マイクロプロセッサ21のRAM21cに保持される。また、これと同時に、指紋画像検出素子11によって、指の指紋画像が取得され、指紋画像処理回路15によって所定の処理が施された指紋データは、マイクロプロセッサ21のRAM21cに記憶保持される(ステップS5)。

【0039】次いで、上記RAM21cに記憶された静

電容量 C_x の大きさに応じた電流が、所定の値または所定に範囲にあるかがマイクロプロセッサ21において比較判断される(ステップS6)。ICカード1の静電容量検出用電極19aおよび/または19bに触れた対象物が生体であるか否かが判断される(ステップS7)。たとえば、静電容量検出回路17の検流回路Dで検出される電流値は、人間の指をコピーした模造品では、人間の指の有する静電容量とは異なった値となるため、生体ではないと判断され不正利用者と判断される(ステップS8)。この場合には、ICカード1内での処理は中止される。

【0040】生体であると判断されると、メモリ16に予め登録されている真正利用者の指紋データがマイクロプロセッサ21のRAM21cに読みだされ、マイクロプロセッサ21のRAM21cに記憶された検出された指紋データとの照合が行われる(ステップS9)。真正利用者の指紋データと検出された指紋データとが合致しているか判断され(ステップS10)、検出されたICカード1の利用者の指紋データと予め登録された真正利用者の指紋データとが合致しない場合には、不正利用者と判断される(ステップS8)。

【0041】検出されたICカード1の利用者の指紋データと予め登録された真正利用者の指紋データとが合致する場合には、ICカード1の利用者は真正な利用者と判断されて、外部機器51とICカード1との間のデータ入出力が許可される(ステップS11)。この結果、マイクロプロセッサ21の制御演算回路21aは、インターフェース回路22とメモリ16との間でデータの受け渡しを行う。これによって、外部機器51とICカード1との間の非接触なデータ通信が可能になる。

【0042】以上のように、本実施形態に係るICカード1によれば、ICカード1の真正な利用者の指紋データをICカード1内に予め登録しておき、ICカード1の利用に際して利用者の指紋画像を検出してICカード1内に取り込み、登録された指紋データと検出された指紋データを照合する構成としているため、ICカードの利用者の真偽を確実に判断することができる。また、本実施形態に係るICカード1によれば、ICカード1内に指紋データを登録保持しており、ICカード1の真正な利用者によって指紋データを管理することができるため、外部機器51の管理者やネットワーク手段によって侵入してくる第三者によって悪用されることがない。また、本実施形態によれば、ICカード1に外部機器51との接続のための外部端子がないため、たとえば、ICカード1を紛失しても、外部端子から登録された指紋データや各種のデータを他人に盗まれることがない。また、本実施形態によれば、指紋データの照合によって、ICカード1の真正な利用者を特定することができるため、たとえば、外部機器51に暗証番号等の入力をする必要がなく、ICカード1の使い勝手が向上する。ま

た、本実施形態によれば、ICカード1の真正な利用者をICカード1内で特定することができるため、真正な利用者の特定のために外部機器51との通信等を行う必要がなく、真正な利用者の特定に要する時間を短縮することができる。また、本実施形態によれば、ICカード1を駆動する電力が外部機器51から非接触で供給されるため、たとえば、ICカード1を紛失しても、外部機器51がなければICカード1を使用することができず、ICカード1の安全性が一層向上する。また、本実施形態によれば、ICカード1を外部機器51に接続する必要がなく、ICカード1の外部機器51への接続作業が省け、また、外部機器51との接続による磨耗等の問題が解消される。

【0043】さらに、本実施形態によれば、ICカード1の指紋画像検出領域Rに設けられた生体検知用の静電容量検出用電極19および静電容量検出回路17によって、指紋画像検出領域Rに触れた対象物が生体であるか否かを検出でき、例えば、指紋データを模した模造品等を用いたICカード1の悪用を防止でき、ICカード1の安全性をさらに高めることができる。また、上記した実施形態では、ICカード1に指紋データの登録のみを行ったが、指紋データの登録と併せて、登録者の指の有する静電容量の値もICカード1内のメモリ16の所定のアドレスに登録しておくことができる。指の状態がウェットである人とドライである人の検出される静電容量は異なるため、指の状態がウェットである人とドライである人の検流回路Dにおいて検出される電流値も異なる。したがって、ICカードの利用時に、利用者の指から得られた静電容量検出回路17の検流回路Dの電流値から、指の状態がウェットであるかドライであるかを判断すれば、指紋データの照合を行う前に、登録者と利用者との照合をある程度大雑把に行うことが可能となり、ICカード1の安全性をさらに高めることができる。

【0044】

【発明の効果】本発明によれば、ICカードの利用者の真偽の判断を外部機器と非接触でかつ確実に行うことができる。また、本発明によれば、ICカードの利用者の真偽の判断に要する時間を短縮することができる。また、本発明によれば、ICカードを紛失したり盗まれても、他人に悪用されることを防止することができる。また、本発明によれば、指紋照合による利用者の真偽の判断を行う機能に加えて、生体検知手段を備えているため、ICカードの安全性がさらに向上する。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るICカードの構成を示す構成図である。

【図2】本発明の一実施形態に係るICカードを実現するハードウェア構成の一例を示す構成図である。

【図3】ICカードの指紋画像検出領域の形成位置の一例を示す図である。

11

【図4】ICカードの指紋画像検出領域の形成位置の一例を示す断面図である。

【図5】静電容量検出回路の一例を示す回路図である。

【図6】指紋画像検出素子の一例を示す図である。

【図7】ICカードの使用法の一例を説明するためのフローチャートである。

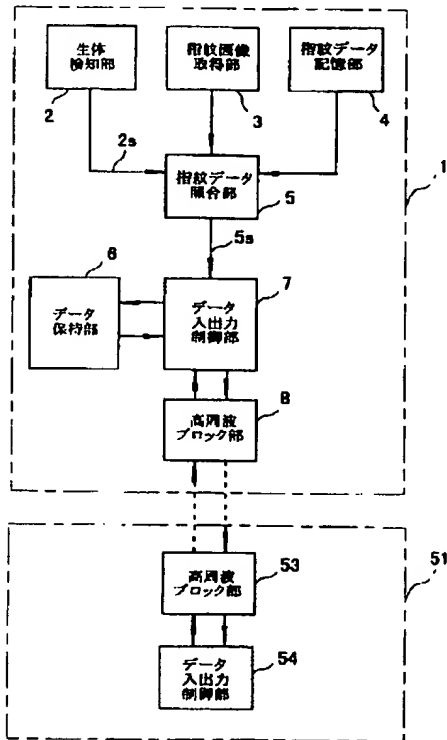
【符号の説明】

12

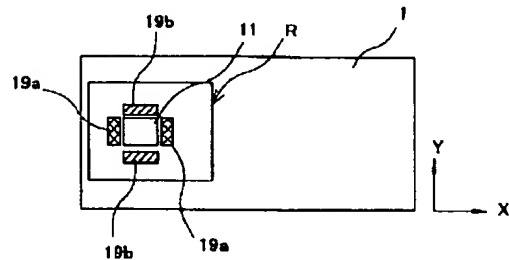
* 1…ICカード、2…生体検知部、3…指紋画像取得部、4…指紋データ記憶部、5…指紋データ照合部、6…データ保持部、7…データ入出力制御部、8…高周波ブロック部、11…指紋画像検出素子、15…指紋画像処理回路、16…メモリ、17…静電容量検出回路、19…静電容量検出用電極、21…マイクロプロセッサ、22…インターフェース回路、23…送受信回路、51…外部機器。

*

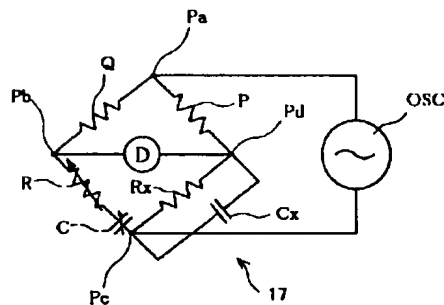
【図1】



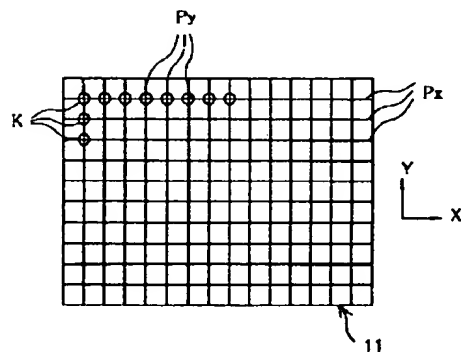
【図3】



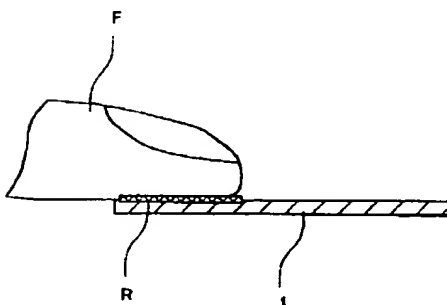
【図5】



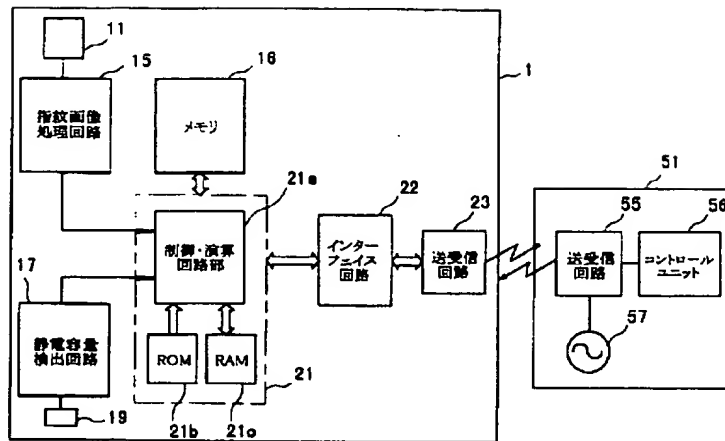
【図6】



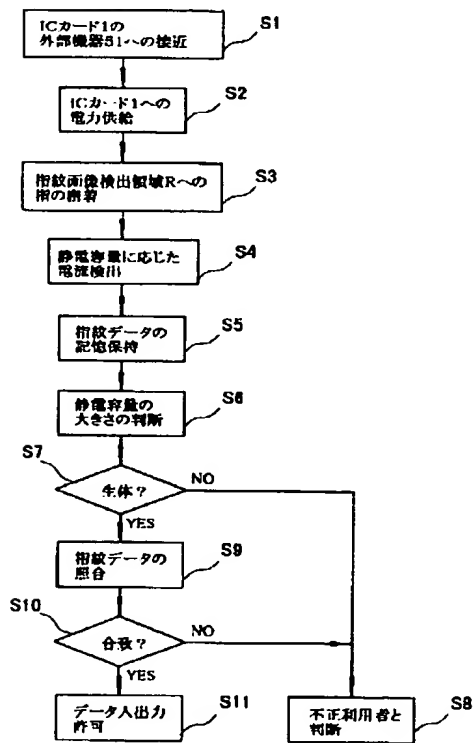
【図4】



【図2】



【図7】



BEST AVAILABLE COPY